

Realtime
publishers

"Leading the Conversation"

The Essentials Series

IT Compliance Volume II

sponsored by

SECURE[®]
COMPUTING

by Rebecca Herold

Article 1: Addressing Government Agency Access and Authentication Challenges	1
The Importance of Authentication and Access Control.....	1
Significant Concerns for Government Information	2
Government Initiatives.....	3
Authentication and Access Control Challenges.....	5
Certification and Accreditation.....	5
Unique Requirements.....	5
Compliance Challenges	6
Implementing Two Factor Authentication.....	6
Don't Overlook Important Components	7
Identity Verification.....	7
Implement a PIV Management Strategy.....	7
Implementing Appropriate Access Controls.....	8
Meeting Compliance Requirements Is Possible	8
Successful Compliance Will Result in Improved Security and Privacy.....	9
Article 2: Addressing Web-Based Access and Authentication Challenges.....	10
Incidents Occur When Controls Are Weak	10
Web Authentication Issues	11
Multi-Factor Authentication	12
Access Control Issues	13
It Can Be Done.....	15
Pairing Multi-Factor Authentication with Access Control Is Effective.....	16
Article 3: How Access Management Compliance Supports Good Business.....	17
Legacy Systems Create Vulnerabilities	18
Protecting Business Operations Is a Basic Management Objective	18
Laws Specifically Require Authentication and Access Controls	19
Address Insider Threats	21
Good Business Has Good Controls.....	22
Article 4: Preventing Data Leakage Through Email and Instant Messaging.....	23
Incidents Occur Easily and Often	23
Consider IM Vulnerabilities	24
Consider Email Vulnerabilities.....	27
Policies and Education Are Very Important	28


Implement policies, procedures and standards	28
Awareness and Training	29
Implement Messaging Security in Depth.....	32
Article 5: Addressing Image Spam	33
What Is Image Spam?	33
Image Spam Negatively Impacts Business	34
Addressing Image Spam Threats	35
Article 6: What Businesses Need to Know About Reputation-Based Messaging Technology.....	37
An Overview of Messaging Filtering	37
What Is Reputation-Based Technology?	38
Features to Look for in a Reputation-Based Spam Filtering Solution.....	39
Article 7: Security Products Must Be Secure	40
Software Vulnerabilities in the Security Products Industry.....	40
Costs Associated with Vulnerable Security Products.....	41
Hardened Security Software Is Necessary to Protect Business	42
Examples of Security Products that Must Be Hardened.....	42
25 Questions to Ask Security Product Vendors.....	43
Article 8: Reducing Attack Exposure for Internet-Facing Applications	47
Build In Security	47
Attack Methods.....	48
Positive Security Models vs. Negative Security Models	49
Negative Security Model	49
Positive Security Model.....	49
Providing Granular Access to Applications.....	50
Assign Access Privileges to Subjects Using Roles.....	51
Configure Access Privileges to Objects Using Roles	51
Restricting Applications Capabilities	52
Get Rid of What You Don't Need	52
Internet-Facing Applications Security Improvement Checklist	53
Article 9: Using Certified Products to Improve Compliance.....	54
What Does "Certified" Really Mean?.....	54
Does Certification Really Mean You Have a Better Product?	55
Different Certifications = Different Meanings	55

Common Criteria	56
ISO/IEC 27001 Certification	58
Certification Assists with Compliance Efforts	58


Article 1: Addressing Government Agency Access and Authentication Challenges

The Importance of Authentication and Access Control

Authenticating users to access enterprise information resources is a critical component of enterprise information security. Creating technologies that authenticate users with a high degree of confidence has always been a challenge not only because of the typical complexity of the systems but also because of the amount of confidence that must be placed within the end user to appropriately secure his or her own user authentication information, most commonly the user ID and password. This challenge increased exponentially as computing moved from the solely centralized mainframe to decentralized enterprise business processing on multiple, business unit managed servers, and then expanded beyond the perimeter into the Internet and systems owned and managed by business partners.


 Why is authentication important? Significant protection of enterprise information resources depends upon knowing the identity of a user of the network and associated systems.

Access control is another critical component for securing enterprise information resources. Access controls must be established to preserve the confidentiality and integrity of information. Confidentiality requires that only authorized users can read information, and integrity requires that only authorized users can alter information in authorized ways. Authorization and authentication are fundamental components of access control.

 Authentication is a process of determining who you are. Authorization determines what you are allowed to do.

Significant Concerns for Government Information


Over the past several years, the U.S. Government Accountability Office (GAO) has identified the historically poor authentication and access control practices as barriers for successful information sharing not only between government entities but also with the private sector. Since 1997, the GAO has recommended the development of a comprehensive plan for information sharing to support critical infrastructure protection efforts. It continues to be a concern. All government agencies must act to address the significant information security weaknesses within their systems and applications. Authentication and access control practices are two key areas to resolve.

 From the GAO's 2007 "High-Risk Series: An Update" which was released on January 31, 2007 (<http://www.gao.gov/htext/d07310.html>): "To improve existing technology protection programs, agencies need to implement the many GAO recommendations that remain unaddressed. In addition, further action is needed. The legislative and executive branches should strategically examine existing programs, evaluate alternative approaches, and develop a comprehensive framework with clear responsibilities and accountability for identifying and protecting critical technologies."

The concerns are validated through numerous incidents that have recently occurred within federal agencies. Just a sampling of them shows how authorization and/or access controls were vulnerable:

- October 12, 2006—Hackers broke into the Congressional Budget Office's mailing list and sent a phishing email message that appeared to come from the CBO.
- August 20 - 22, 2006—A security breach in the William D. Ford Federal Direct Loan Program within U.S. Department of Education and Federal Student Aid exposed private information of student loan borrowers during a computer software upgrade. Users of the Direct Loans Web site were able to view personal information, including Social Security numbers, of others.
- August 23, 2006—A faulty Web site software upgrade resulted in the exposure of personal information of 21,000 student loan holders on the U.S. Dept. of Education Direct Loan Servicing Online Web site. Information included names, birthdates, Social Security numbers, addresses, phone numbers, and in some cases, account information.

There are also significant concerns with state and local level government agencies. According to a paper released December 21, 2004 by the National Association of State Chief Information Officers (NASCIO), "Who Are You? I Really Wanna Know: E-Authentication and its Privacy Implications," some of the most critical factors impacting information security within the government are authentication and access controls.

 E-authentication within the NASCIO report refers to the process of establishing the identity of individuals involved in transactions over the Internet. Get the report from <http://www.nascio.org/publications/documents/NASCIO-WhoAreYouEAuthBrief122104.pdf>.

The report stresses the need to address authentication risks involved with putting applications and systems on the Internet, raising the awareness of the people authenticated, limiting the amount of personal information used for authentication purposes, and understanding the benefits and risks of identifiers. The concerns are well-founded, as the following examples demonstrate.

At the state level:

- July 16, 2006—The Mississippi Secretary of State’s Web site listed more than two million Uniform Commercial Code (UCC) filings in which thousands of individuals’ Social Security numbers were exposed.
- June 29, 2006—A hacker broke into a Nebraska Treasurer’s Office child-support computer system containing names, Social Security numbers, and other information such as tax identification numbers for 9000 businesses.


At the local level:

- November 16, 2006—The Carson City, Nevada Sheriff’s Department reported that at least 50 residents had their credit card information stolen from the department’s systems by employees of local businesses.
- November 7, 2006—Hackers broke into the City of Lubbock, Texas’ Web site and compromised the online job application database, which included Social Security numbers.
- October 23, 2006—An official from the Illinois Ballot Integrity Project says his organization gained unauthorized access into Chicago’s voter database containing the names, Social Security numbers, and birth dates of 1.35 million residents.
- September 20, 2006—The City of Savannah, Georgia’s Web site exposed personal information, including name, address, driver’s license number, vehicle identification number, and Social Security number, online for 7 months because of improperly configured access controls on the firewall.


Government Initiatives

Over the past few years, there have been various laws and executive orders specifying the actions necessary to improve information sharing for government agencies, particularly since September 11, 2001. Just a few of these include:

- The Homeland Security Act of 2002 required procedures for facilitating homeland security information sharing and established authorities to share different types of information, such as grand jury information; electronic, wire, and oral interception information; and foreign intelligence information.
- The Critical Infrastructure Information Act of 2002 required the establishment of uniform procedures for the receipt, care, and storage of critical infrastructure information that is voluntarily submitted to the federal government.
- The Electronic Government (E-Government) Act of 2002 was designed to enhance the management and promotion of electronic government services and processes and to increase the electronic availability of information to the public. It established the Office of E-Government within the Office of Management and Budget, authorized the use of nearly \$350 million over 4 years to fund e-government initiatives, expanded the use of share-in-savings contracts for information technology, and created a statutory chief information officers council.

 The E-Government Act of 2002 is located at <http://thomas.loc.gov/cgi-bin/query/D?c107:5:./temp/~c107F0ctv1>.

-
- Federal Information Security Management Act (FISMA) of 2002 was passed into law as part of the E-Government Act. Its goals include development of a comprehensive framework to protect the government's information, operations, and assets. FISMA assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB), in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers, and Inspectors General (IGs) to conduct annual reviews of the agency's information security program and report the results to OMB.

 The Federal Information Security Management Act of 2002 is located at <http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3844>.

- The Homeland Security Presidential Directive 12 (HSPD-12) of 2004 requires a common identification standard using two-factor authentication for federal employees and contractors for gaining physical access to controlled facilities as well as logical access to controlled information systems.

 HSPD-12 is located at <http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>.

International initiatives, data sharing, and associated requirements have also heightened the need for better security and strengthened authentication and access controls. For example, the U.S. and other members of the Financial Action Task Force (FATF), an inter-governmental policy-making body created to develop and promote national and international policies to combat money laundering and terrorist financing, have attempted to address these issues in a global context by adopting international standards. FATF Special Recommendation VII requires countries to mandate that cross-border funds transfers of more than a specified amount contain accurate and meaningful information about the person originating the transfer. This information must include:


- Name of the originator
- Location of the account
- Account number, if one exists, or a unique reference number
- Address of the originator, or national identity number, customer identification number, or date or place of birth if the country permits

Authentication and Access Control Challenges

Implementation of effective authentication and access controls to meet the requirements of these various laws and directives will be challenging to all government agencies. The challenges must be met with thorough and careful planning.

Certification and Accreditation

Government agencies must have their information security programs certified and accredited. The National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), establishes the minimum national standards for certifying and accrediting government agency security systems. This process provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the Information Assurance (IA) and security posture of a system or site. Security test and evaluation validates the correct implementation of identification and authentication, audit capabilities, access controls, object reuse, trusted recovery, and network connection rule compliance. Individual tests evaluate system conformance with the requirements, mission, environment, and architecture as defined in the System Security Authorization Agreement (SSAA).

 The National Information Assurance Certification and Accreditation Process (NIACAP) is located at http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf.

Unique Requirements

Some laws that government agencies must follow have very specific and unique information security requirements. Consider HSPD-12 in particular. The NIST Computer Security Division developed Federal Information Processing Standard (FIPS) 201 Personal Identity Verification (PIV) of Federal Employees and Contractors to satisfy the requirements of HSPD-12.

 FIPS 201 is located at <http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>.

At a high level, FIPS 201 standards require agencies to:

- Properly protect the personal privacy of all subscribers of the PIV system
- Authenticate identity source documents to obtain the correct legal name of the person applying for a PIV card
- Electronically obtain and store appropriate biometric data, such as fingerprints and facial images, from the PIV system subscriber
- Create a PIV card that is personalized with data needed to grant access to the subscriber to federal facilities and information systems
- Assure appropriate levels of security for applications and access to information
- Provide interoperability among federal organizations

There are many issues involved with implementation of the standards. Just a few of the issues CIOs must consider include:

- HSPD-12 and FIPS 201 compliance activities are unfunded mandates. Costs may be significant.
- Background checks must likely be performed on most, if not all, existing employees and contractors, along with the ongoing costs for these activities.
- Replacement IDs must likely be issued for most, if not all, existing employees and contractors, along with the ongoing costs for issuing new IDs.
- Badge scanners for buildings and individual computers will need to be chosen, purchased, and implemented. It is likely most agencies will need to upgrade systems and modify applications to handle the cards.

Compliance Challenges

Implementing Two Factor Authentication

There will be challenges to meeting the authentication requirements of these standards. Historically, the most common method of authentication was using a password or personal identification number (PIN). This typically was the only component necessary in conjunction with the ID to authenticate; called “single factor authentication.” This was the “something you know” component of authentication.

Other components of authentication can include either “something you have,” such as a driver’s license or smart card, or “something you are,” such as a type of biometrics. Using two of these three components is commonly called two-factor authentication. HSPD-12 requires two-factor authentication in addition to using “secure and reliable identification.”



The standard single factor username/password or PIN authentication method can no longer provide adequately secured authentication. The availability of sniffers and password/PIN cracking tools used to defeat single-factor authentication has removed accountability for the activities that occur through the ID. In addition to these tools, bad habits, such as users choosing easy-to-guess passwords or writing down and leaving passwords in conspicuous places, also put secure authentication of the actual individual at risk.

Using two-factor authentication significantly enhances security by ensuring that all authentication must be carried out using this additional component that only the user is supposed to possess, making the user accountable for the actions on the system and removing the ability for freely available tools to be used to defeat the authentication system.

Don't Overlook Important Components

Organizations must remember that authentication issues go beyond the network perimeter:

- Organizations will need to implement additional components, such as PKI readers, fingerprint readers, or other mechanisms, on mobile computers and mobile media devices to meet the two-factor authentication requirement.
- Remote access components will need to be changed to incorporate two-factor authentication.
- Business continuity plans and tools must account for supporting two-factor authentication and strong access controls.
- Reporting, logging, and audit capabilities must exist to indisputably document all access attempts into the network as well as resources that were accessed upon successful authentication.

Identity Verification

Typically birth certificates, passports, and visa applications were used to verify the identities of individuals when authorizing them to access government systems and applications. The September 11, 2001 attacks raised concerns about the integrity of identity documents such as passports and visa applications because the terrorists responsible for the attacks reportedly used such documents to board the planes that were hijacked. HSPD-12 requires secure and reliable identification that:

- “Is issued based on sound criteria for verifying an individual employee’s identity
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Is issued only by providers whose reliability has been established by an official accreditation process.”

Implement a PIV Management Strategy

Agencies need to establish a sound PIV management strategy. They need to create an effective user ID enrollment procedure as well as well-defined and documented issuance and management procedures. This is not just an electronic information logical access issue. Agencies must also implement procedures to control physical access to areas where information on the network is accessed and where physical information processing resources, such as servers, are located. These procedures must include how to terminate these logical and physical access authorizations.

Implementing Appropriate Access Controls

To be most effective and cost efficient, the chosen access control system should have components able to integrate each authorized individuals' access to physical and logical resources. The system should

- Be compatible with the physical facility security devices, such as parking gates, building entrances, and so on
- Control logical access to all types of network resources, such as databases, workstations, applications, and so on
- Be able to restrict access to only the resources necessary to perform job responsibilities; this will typically consist of being able to establish access privileges through such mechanisms as Access Control Lists (ACLs)

Meeting Compliance Requirements Is Possible

Meeting compliance requirements with all the many laws and regulations can seem overwhelming, and sometimes impossible. However, it can be helpful to look at an organization that has succeeded in meeting this compliance challenge. Orange County, California is a good case in point.

Orange County's network delivers a wide range of services to public agencies throughout the county. Each county agency is responsible for managing their own user IDs and associated access controls but they each need access to certain services and resources on the core network, such as mainframe data, terminal services, and other custom applications.

A challenge for Orange County network administrators was the inability to restrict and track access of additional connections once outside agencies had made the initial connection with the core terminal server. Synchronization with the scattered agency systems was critical to ensure that user data was properly shared between agencies, minimizing redundant data, and reducing the cost and resources necessary to maintain data across several systems.

After careful consideration and risk analysis, Orange County established several key requirements:

- Create a single portal entry point into the network.
- Deploy and enforce a centralized information resource access policy from users in outside agencies.
- Establish and implement a centralized user domain in Microsoft Active Directory (AD) that leverages data from each outside agency's existing AD systems.
- Implement a single sign-on (SSO) capability to reduce the number of logins needed throughout the network for users from outside agencies.

Orange County implemented SafeWord SecureWire from Secure Computing (<http://www.securecomputing.com>) to

- Connect the outside agencies to the centralized network through a single portal
- Create an enterprise-wide, policy-driven access control system with SSO for applications
- Standardize the authentication protocols, utilizing tokens for the two-factor authentication
- Create audit trails to track and enforce access policies for each individual within the central outside agencies
- Manage the existing infrastructure using AD tools

Successful Compliance Will Result in Improved Security and Privacy

The old information security practices typically used within most government agencies are not only inadequate for today's new security threats, as a review of recent incidents demonstrates, they also will not meet the many new legal requirements. It is time to strengthen security and better protect information security and privacy within government agencies.

When implementing authentication and access control compliance solutions, it will be important to:

- Understand the information security and privacy risks associated with different methods of authentication.
- Choose authentication methods to minimize information security and privacy risks consistent with the need for security in a transaction, due to the flow of personal information in the process of authentication.
- Conduct risk assessments to establish appropriate levels of authentication for different transactions.
- Understand the importance of cross-boundary cooperation when different jurisdictions are involved in authentication.
- Involve IT specialists, information security specialists, and privacy specialists in designing authentication systems.


Article 2: Addressing Web-Based Access and Authentication Challenges

Incidents Occur When Controls Are Weak

Many incidents occur through access and authentication vulnerabilities. Let's look at some highlights of a recent event that may have been the result of such weaknesses.

- Sometime in December 2006, TJX Companies Inc. discovered vulnerabilities in their computer systems and networks that allowed unauthorized access to their data, including their customers' personally identifiable information (PII).
- On January 17, 2007, TJX announced its computer network that handles customer transactions for around 2500 retail stores was hacked into, and PII, including credit, debit, and driver's license information, was stolen.
- On January 22, the Massachusetts Bankers Association (MBA) said that banks had to cancel and reissue cards affected by the breach and that the banks that issued the cards, rather than individual consumers, would cover all fraudulent purchases.
- On January 24, the MBA said that fraudulent use of the stolen debit and credit card information from the TJX breach had been reported by banks in Florida, Georgia, and Louisiana, as well as overseas.
- On January 29, AmeriFirst Bank in Alabama bank filed a federal class action lawsuit in Massachusetts against TJX in an attempt to recover the costs of a breach incident the bank alleged was the result of negligent data security practices by TJX.
- On January 29, a complaint seeking class action status was filed in federal court in Massachusetts on behalf of all TJX customers in the United States against TJX for negligently failing to adequately secure its customer information. The single count common law negligence complaint alleges TJX did not comply with the Payment Card Industry Data Security Standard (PCI DSS).

As you can see, this breach impacted many entities: TJX, their business partner banks and retailers, credit card companies, and customers. And the fallout continues. Not complying with the PCI standards can also result in fines on merchant banks and retailers. And there are many other federal and state-level laws and regulations that may also be applied, such as the Gramm-Leach-Bliley Act (GLBA) and the FTC Act, to name just a couple.

 VISA imposed \$4.6 million in fines in 2006 for PCI noncompliance, up from \$3.4 million in 2005.

There have been many other incidents that resulted from exploiting weak authentication and access controls. Organizations must ensure applications and systems are built using strong information security practices. If they aren't, the impact could not only be huge, it could linger on for many years, or even close the business.

This paper focuses on two important aspects of applications and systems security—authentication and access controls. Business leaders must ensure they are implemented effectively to help protect the business as well as PII.

Web Authentication Issues

Significant security vulnerabilities can exist if Web applications do not implement authentication mechanisms appropriately. The issues differ for authentication for those who only occasionally use the application, those who regularly use the application, and those who must provide support to the application.

Historically, single-factor authentication, in the form of an identifier and password, was used for Web authentication. However, there are several realities that make single-factor authentication quite vulnerable to defeat:

- Passwords can be inappropriately shared with others. Check the monitors for sticky notes within most organizations and you will likely find several passwords; not to mention the executive assistant to the VPs who has a nicely documented list of all their passwords and identifiers by his keyboard.
- Most people create poor passwords that can be easily guessed, whether by chance or through the use of any number of freely available password crackers.
- Clear-text passwords in transit are vulnerable. There are a large number of clever communications eavesdropping tools available to collect passwords as they pass through network transmissions.
- Encrypting passwords in transit doesn't provide comprehensive protection. Keystroke loggers are increasingly used to record passwords and then send them to criminals to use to gain access.
- Clear-text passwords in storage are vulnerable. If there are weaknesses in the system housing the passwords, hackers may be able to get to the password file.
- Single-factor authentication implementations can be vulnerable to man-in-the-middle and Denial of Service (DoS) attacks.

The U.S. government saw these risks and reacted to protect consumer PII by recently requiring banks to implement multi-factor authentication on their Web sites. The Federal Financial Institutions Examination Council (FFIEC) considers single-factor authentication as inadequate for transactions involving PII, and on October 12, 2005, issued updated guidance requiring financial institutions engaging in any form of Internet banking to use effective methods to authenticate the identity of customers using those products and services. Based upon the result of risk assessments, financial institutions must implement multi-factor authentication, layered security, or other controls reasonably configured and implemented to mitigate those risks.

 The FFIEC Interagency Guidance on Authentication in an Internet Banking Environment can be found at http://www.ffiec.gov/ffiecinfobase/resources/info_sec/2006/ots-ceo-ltr-228.pdf.

Multi-Factor Authentication

To implement multi-factor authentication, at least two of the following three items are used with the identifier to authenticate:

- Something you have, such as a security token, credit card, proximity badge, and so on
- Something you know, such as a password, PIN, passphrase, and so on
- Something you are; a biometric attribute, such as your fingerprint, voice pattern, retinal scans, and so on

There are challenges in implementing a multi-factor authentication solution for Web applications. Just a few include:

- Deploying the “something you have,” such as security tokens, to all users. This may be a significant undertaking for an organization that wants to deploy to all their customers.
- Successfully and effectively communicating to a diverse group of users how to be able successfully use the security tokens they receive.
- Deploying the “something you are” factor may not be feasible for some organizations to use with their customers, depending upon the numbers involved and how much support they can make available to the customers.
- Using multi-factor authentication could cost a significant amount of money to deploy.

Most organizations deploying multi-factor authentication determine that using passwords or PINs in combination with a security token is the best solution to meet multi-factor authentication requirements.

Access Control Issues

Once an individual is authenticated, you must be sure to limit the individual's access to only those systems and applications resources for which the user is approved. User accounts must be given the least privileges necessary not only to provide strong security to protect systems and information resources but also to meet the growing numbers of laws and regulations that require least privilege access. Just a couple of U.S. laws that have this least privilege requirement include GLBA and the Health Insurance Portability and Accountability Act (HIPAA), in addition to the FFIEC guidance discussed earlier.

Organizations must address multiple issues for Web-based application access controls. A comprehensive security policy utilizing a system that centralizes management can be implemented to be successful with access control efforts. A comprehensive and effective Web access solution should have the capabilities for:

- Endpoint security and configuration compliance enforcement and reporting capabilities—Inappropriately configured servers, as well as remote devices, create threats to the organization's systems and information resources; malware could enter the organization, unpatched systems could be exploited and have a chain reaction impact to the internal systems, and so on. There should also be ways to ensure each system has the latest software releases and complies with corporate firewall and security policies.
- Centralized access management to protect intranet and extranet resources—You should be able to establish least privilege and role-based access through one utility to be most efficient, not leave security holes, and ensure appropriate access settings and security.
- Centralized policy reporting—Organizations often have to run multiple reports for each of the many access points to their network. An effective solution will be able to pull all audit logs and reports together for more efficient reporting and review as well as to create the documentation necessary to comply with multiple laws, regulations, and contractual requirements.
- Centralized policy enforcement—Ensuring all applications and servers have been appropriately updated to meet new policies and address new threats can take a significant amount of time. An effective solution will be able to ensure the policy updates are distributed to all servers and systems, significantly easing the policy update activities.
- Anywhere, anytime remote access to applications, data, and networks. With customers, personnel, and business partners scattered all over the world, limiting the time applications are available is no longer an option for most businesses.

Some of the basics for Web application authentication and access control security include:

- Limiting the services offered by the computer running the Web server to a minimum
- Limiting the number of users with most privileged access, such as Administrator in NT or root in UNIX, to a minimum
- Limiting the number of accounts on each system to the minimum needed
- Performing regular risk analysis and vulnerability assessments
- Changing the default settings on systems to more secure settings
- Applying security patches on a timely and ongoing basis
- Logging key events—such as failed and successful logins, attempts to access files/directories without authority, successful and failed attempts to access sensitive data—to help ensure accountability and for troubleshooting purposes



Logs often contain sensitive information such as dates and times of user access. Logs containing sensitive information should be accessible only to authorized staff and should not be publicly accessible.

- Removing all sample scripts from Web servers and Web development tools; they often contain well-known security holes that potential intruders try to exploit
- Checking regularly to ensure sensitive data files were not created within temporary directories by Web development tools as a side effect
- Encrypting sensitive data collected through the Web application, accessed by the Web application, or stored on the Web server



Some versions of SSH1 are vulnerable to a buffer overflow in the authentication phase of establishing a SSH tunnel. Snort rule 1327 will identify this ssh-crc32exploit.

It Can Be Done

Although there are challenges, Web application authentication and access controls can, and must, be deployed securely. Organizations have succeeded. Regional MLS (RMLS), a real estate multiple listing service (MLS) in Florida, is a case in point. IDC did a case study of RMLS' Web authorization and access security implementation.

 View the IDC RMLS case study at http://www.securecomputing.com/pdf/SS_RegionalMLS-IDC.pdf.

Real estate professionals possess a great amount of PII, along with sensitive information about real estate details, which must be kept from public access. Controlling access to the MLS, transaction management systems, and broker systems, has become increasingly critical because it is no longer simply the listing information that is at risk. Concern for privacy and preventing data breaches must be a priority for real estate professionals.

MLS systems typically include contact management and CRM applications that store PII about clients and prospects. RMLS is subject to federal regulations such as the Sarbanes-Oxley Act (SOX) and GLBA that require safeguards to protect this confidential customer data.

RMLS had observed that their MLS subscribers, including the agents, secretaries, and assistants, were often sharing their systems identifiers and passwords with many other third parties. RMLS realized that these activities put the PII within their systems at great risk, and put them in noncompliance with applicable laws and regulations. They determined that the most effective way to address this was to use a centrally managed access control system in conjunction with an authentication method that would involve passwords that could not be shared.

To address the regulatory requirements and the vulnerable security practices, RMLS did some research and began deployment of more than 17,000 security tokens for multi-factor authentication to their MLS subscribers in the summer of 2005 as part of their implementation of Clarity's SAFEMLS security access control system paired with Secure Computing's SafeWord PremierAccess authentication technology.

 Find information about the Clarity Security SAFEMLS system at <http://www.safemls.com/>. Find information about the Secure Computing SafeWord PremierAccess authentication technology at <http://www.securecomputing.com/index.cfm?skey=643>.

RMLS reported the deployment was successful and that the subscribers were happy with the solution. No cost was passed on to the subscribers for the tokens, unless they lost one and had to replace it. During implementation, all users were required to pick up their tokens from the RMLS facility. Before they were issued tokens, they had to attend a 30-minute security training session. Since the initial roll-out, RMLS sends new users security information and gives them the option of either picking up their token at their facilities or receiving it by mail.

Pairing Multi-Factor Authentication with Access Control Is Effective

Multi-factor authentication removes most of the risks involved with just using a password. Using security tokens as the multi-factor authentication solution of choice provides protection against:

- Transmission eavesdropping
- Keystroke loggers and replay
- Online guessing
- Impersonation and spoofing
- Man-in-the-middle attacks
- Session high-jacking

Implementations using security tokens that integrate with centralized access controls work well to help prevent many kinds of security compromises while addressing regulatory and contractual requirements to protect sensitive information. With thoughtful planning, implementation can be efficient and effective, even with end users who are geographically dispersed.

Article 3: How Access Management Compliance Supports Good Business

Many business leaders I speak with now have great concern for data protection law and regulation compliance, which is certainly prudent. However, often when digging into the details of their compliance plans and activities, I find most of the effort and budget is going towards initiatives for firewall and perimeter protection, with increasing implementations for encryption.

These are definitely important! But when I ask about any plans they have for improving their authentication methods, a large number, with perhaps the exception of the online banks, say something similar to, “Oh, we are comfortable with our current authentication solution; our passwords must be strong, and must change every 90 days. And we have not experienced any problems with our access control systems. So, we should already be in compliance with these types of legal requirements.” But will single-factor re-usable passwords continue to be an acceptable practice for authenticating enterprise users as incidents continue to occur on an ever more frequent basis?

Similarly, when I ask about plans for improving access control methods, many business leaders have a response similar to, “Our access controls are based upon departmental responsibility and manager oversight. We have used this method for several years. It seems to work fine, and we have trust in our managers’ capabilities.” Will the old way of establishing and managing access controls still be acceptable as the insider threat continues to negatively impact businesses and their customers? Will these practices pass muster with regulatory oversight agencies that check for compliance?

Legacy Systems Create Vulnerabilities

Systems and applications created two and three decades ago are still being used, typically to support the newer systems and applications installed. Effort goes to the new systems and technologies, but security of legacy systems is often not updated to address the new vulnerabilities created by new systems and applications connected to the legacy systems. A good example of the vulnerabilities from legacy systems comes from the State of Wisconsin 2006 financial audit:

Condition:

The provider system was developed in the early 1990s and has not been able to easily accommodate changes that have occurred over time, which has resulted in errors occurring within the system. Fund staff estimate approximately 15 to 20 hours a week are needed to address the problems that have developed. Further, these system issues have also limited the Fund's ability to address system access control weaknesses.

Effect:

The aging system presents an increased risk to the integrity of the Fund's financial operations. Access control weaknesses increase the risk that unauthorized or erroneous changes could be made to provider system data without being detected. In addition, increased time spent to correct processing problems that arise with the current system results in less time available for more productive tasks for the Fund.

This situation is very similar to the situations within a large portion of businesses. Businesses have valid reasons to keep old legacy systems to continue providing processing power, storage repositories, and back-office functions. However, along with the decision to keep the legacy systems comes the decision to maintain the security controls of these old systems to an acceptable level. Not only is this necessary to protect business assets but also it required through numerous laws and regulations.

Protecting Business Operations Is a Basic Management Objective

Protecting the resources that provide critical business operations is a basic management objective for every organization. This objective is realized largely by designing and implementing controls that prevent, limit, and detect unauthorized access to computing resources, programs, and information. Electronic access controls include user identification and authentication, authorization, boundary protection, cryptography, and auditing and monitoring of security-related events.

Network and applications activities must be linked to specific individuals to create accountability, provide a history of the activities, and to catch inappropriate activities. Using identifiers that are unique to each user links the accountability of activities to a specific individual. Appropriate access, and subsequently accountability, can then be assigned to individuals using the identifiers. Too many times within organizations, the authentication and access control policies and supporting processes are implemented in ways that lose the important accountability and history components.

A few excerpts from the August 2006 GAO Audit Report for the Centers for Medicare & Medicaid Services (CMS—available at <http://www.gao.gov/new.items/d06750.pdf>) demonstrate how proper authentication and access controls are often lacking. I have highlighted a few sentences that seem to be a problem for all organizations throughout all industries:

*Although CMS has many information security controls in place that are designed to safeguard the communication network, there were significant weaknesses in electronic access controls and other controls designed to protect the confidentiality, integrity, and availability of the sensitive, personally identifiable medical information it transmits. Our review of the communication network revealed 47 weaknesses in electronic access controls and other controls. **A key reason for these weaknesses was that CMS did not always ensure the effective implementation of its security policies and standards.** As a result, sensitive, personally identifiable, medical data traversing this network are vulnerable to unauthorized disclosure, and these weaknesses could lead to disruptions in CMS operations.*

*CMS did not ensure that its contractor adequately identified and authenticated users responsible for managing the communication network. **For example, CMS's contractor did not enforce sufficiently complex passwords for access to certain network devices.** This increases the risk that unauthorized users could gain access to CMS systems and sensitive information.*

***CMS did not ensure that its contractor sufficiently restricted network access and privileges to only those users and processes requiring them to perform authorized tasks.** For example, CMS's contractor did not adequately restrict access paths on certain network devices. In addition, the contractor had several sensitive world-writable files on network management servers, granting inappropriate privileges to these files. These conditions provide more opportunities for an attacker to escalate their privileges and make unauthorized changes to files.*

Laws Specifically Require Authentication and Access Controls

Growing numbers of systems, technologies, network tools, and applications are used throughout the enterprise to enable or streamline business: Web site applications, proxy server firewalls, databases, email servers, data-mining applications, customer relationship management tools, and a seemingly infinite number of other types of business applications. Each of these must effectively enforce authentication and access controls in one way or another. However, many times they do not.

Authentication and access control weaknesses are seen in the findings of almost every information management audit. These weaknesses are also in the findings of almost every regulatory compliance audit. Dealing with authentication and access controls in a consistent, well-documented manner addresses these specific requirements within numerous laws, and results in removing those findings from many different audits, in one fell swoop, saving the business from penalties and fines.

The following table shows just a few of the laws that require authentication and access controls, and the variety of regulatory oversight groups involved.

Law	Sample excerpts requiring authorization and access controls	Covered entities	Regulatory oversight agency
Gramm-Leach Bliley Act (GLBA)	“§ 6801. Protection of nonpublic personal information (b) Financial institutions safeguards... (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.”	All financial institutions regulated by the U.S. Office of the Comptroller of the Currency (OCC)	U.S. (OCC)
Health Insurance Portability and Accountability Act (HIPAA)	“§ 164.312 Technical safeguards. (d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.”	U.S. healthcare providers, insurers, and clearinghouses.	U.S. Department of Health and Human Services (HHS)
21 CFR Part 11; Electronic Records and Electronic Signatures	“Subpart B—Electronic Records § 11.10 Controls for closed systems. (d) Limiting system access to authorized individuals.”	Companies, such as pharmaceuticals, regulated by FDA	U.S. Food and Drug Administration (FDA)
European Union (EU) Data Protection Directive 95/46/EC	“Article 17 Security of processing 1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.”	All Companies conducting business in EU member nations	EU Data Protection Supervisor and the EU country-specific privacy commissioners
Canada’s Personal Information Protection and Electronic Documents Act (PIPEDA)	“4.7 Personal information shall be protected by security safeguards appropriate to the sensitivity of the information. The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.”	All organizations that have personal information about Canadian customers and employees.	Canadian Privacy Commissioners
Japanese Personal Information Protection Law	“Security Safeguards Principle: To prevent loss or unauthorized access, destruction, use, modification or disclosure of Personal Data, Data Collectors must implement security safeguards and provide proper supervision of employees and any other entities to which Personal Data may be entrusted.”	Japanese private businesses	Japanese Government

Address Insider Threats

There are inherent risks in giving personnel access to sensitive information or the capability to perform network and applications administration. According to the 2006 11th Annual CSI/FBI Computer Crime and Security Survey (http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml), 68 percent of organizations experienced security incidents from insiders. According to the Association of Certified Fraud Examiners (ACFE) 2006 report on occupational fraud and abuse (<http://www.acfe.com/documents/2006-rttn.pdf>):

- More than 30 percent of occupational frauds are committed by employees in the accounting department
- More than 20 percent are committed by upper management or executive-level employees
- More than 14 percent are committed within the sales department

Personnel at all levels of the company have the potential to do bad things; appropriate controls must be implemented from the very highest positions down through the rest of the enterprise to help prevent incidents caused by insiders. There have been many published accounts of such incidents. The following is just one example.

On December 19, 2006, a Medco Health Solutions, Inc. computer systems administrator, Andy Lin, was indicted by a federal grand jury in the U.S. District Court for the District of New Jersey for attempting to disable his employer's corporate computer servers through the use of a concealed malicious software program. On or about October 3, 2003, Lin modified existing computer code and inserted new computer code (destructive code) into pre-existing scripts on the Medco Servers, which collectively were designed to delete the patient-specific drug interaction conflict database as well as databases identifying subscribers, plan coverage, prescription administration, and billing data. Part of the new computer code Lin programmed and inserted included a script designed to deploy the destructive code automatically on April 23, 2004, Lin's birthday. On or about January 1, 2005, a Medco computer systems administrator investigating a system error discovered the destructive code embedded within other scripts on the Medco Servers. Medco IT security personnel subsequently removed the destructive code.

Given the sensitivity and criticality of the business resources to which insiders have access and the large amount of money at stake for business processes and electronic resources, access must be controlled, logged, and audited. Compensating controls must exist, such as reviewing logs regularly to ensure insiders are not doing bad things and establishing code review procedures to ensure malicious code is not being put into production.

You will never be able to completely remove the insider threat. However, you can ensure that the access each person has matches, and does not exceed, the access the person actually needs.

Good Business Has Good Controls

Business leaders must address information risks in a comprehensive manner and not just focus on the issues that are the most exciting to work with or that are advertised the most.

Authentication and access controls are some of the least glamorous issues to tackle, but if you fail to do so, information cannot be successfully secured and business is highly vulnerable to be given a harsh blow. When making your business decisions remember:

- New and old systems and applications mixed together create vulnerabilities that must be addressed
- Laws and regulations require business resource authentication and access controls
- Strong authentication and access controls lessen the risk of insider fraud, theft, and crime
- Strong authentication and access controls demonstrate due diligence and support legal actions
- Comprehensive security programs make business more efficient and profitable by preventing incidents and avoiding fines and penalties


Business environments are constantly changing as more users, business partners, systems, and applications are added to the business mix. Organizations must implement a comprehensive and effective information security program that protects business resources while meeting applicable compliance requirements within the context of their business objectives. Business leaders must ensure that the vital authorization and access control policies, procedures, and tools are not overlooked. Consistently applying strong access management is not only good business practice and necessary for compliance, it is vital to business success.

Article 4: Preventing Data Leakage Through Email and Instant Messaging

Incidents Occur Easily and Often

Incidents continue to accumulate and hit the daily headlines. Many of them involve the loss of sensitive information through some type of messaging activity. The losses can have devastating impacts to business.

A large financial organization I once did work for was going through downsizing. They notified their systems administrators 2 weeks in advance of their impending layoff, but allowed them to continue performing their job responsibilities as usual until their last day. Indeed this was not a good idea; 2 weeks following the last day, one of the terminated administrators accessed the internal Web site remotely using the admin ID he was once responsible for, changed the passwords for all the remaining admin IDs, then sent messages to all the other email accounts with a very explicit rant about how horrible the company's security was in addition to posting copies of all email messages on the email server to multiple Internet sites. Although this incident happened several years ago, copies of the email messages still continue to pop up on miscellaneous sites from time to time, much to the embarrassment of the organization, which estimated significant lost customers and associated revenues as a result.


 It is very difficult, and usually impossible, to completely recover information once it has been posted on the Internet.

Insiders pose significant threats to organizations. It is particularly easy to leak sensitive company information and secrets along with personally identifiable information (PII) through messaging technologies such as email and instant messaging (IM).


From the 2005 CERT/Secret Service Insider Threat Study Report (http://www.secretservice.gov/ntac/its_report_050516.pdf):

"An application developer, who lost his IT sector job as a result of company downsizing, expressed his displeasure at being laid off just prior to the Christmas holidays by launching a systematic attack on his former employer's computer network. Three weeks following his termination, the insider used the username and password of one of his former coworkers to gain remote access to the network and modify several of the company's web pages, changing text and inserting pornographic images. He also sent each of the company's customers an email message advising that the website had been hacked. Each email message also contained that customer's usernames and passwords for the website. An investigation was initiated, but it failed to identify the insider as the perpetrator. A month and a half later, he again remotely accessed the network, executed a script to reset all network passwords and changed 4,000 pricing records to reflect bogus information. This former employee ultimately was identified as the perpetrator and prosecuted. He was sentenced to serve five months in prison and two years on supervised probation, and ordered to pay \$48,600 restitution to his former employer."

It is so easy to lose information through messaging paths.

 In February 2006 it was widely reported that the names and Social Security numbers of about 27,000 Blue Cross and Blue Shield of Florida current and former employees, vendors, and contractors were sent by a contractor to his home computer in violation of company policies. The contractor had access to a database of identification badge information and transferred it via email to a home computer.

Messaging systems are vulnerable to hacking from outsiders if not configured appropriately and can be purposefully used for sending sensitive data to outside entities and storage areas. There are also many mistakes made that have resulted in inadvertently sending sensitive information to people and/or systems that should not get such information.


 In November 2006, the personal information and Social Security numbers of 561 Virginia Commonwealth University (VCU) students were accidentally included in two attachments in an email sent to 195 students to inform them about their eligibility for scholarships from Phi Kappa Phi, a national honor society. The information included names, Social Security numbers, local and permanent addresses, and grade-point averages. This was the second time in 2006 that VCU had an incident exposing PII; in September, the names, Social Security numbers, and email addresses of about 2100 current and former students had been online for 8 months because of human error.

The growing use of IM within the business enterprise also opens business to a vast array of threats.

Consider IM Vulnerabilities

IM is increasingly being used within businesses. The implementation and use of IM can create huge vulnerabilities within the enterprise if not implemented appropriately. According to a February 2006 survey of more than 200 U.K. businesses done jointly by Peapod and FaceTime Communications, most organizations are not managing IM and are not protecting their networks from spyware threats that exploit IM vulnerabilities. The survey reported:

- 73 percent of the survey participants had experienced a spyware attack through IM in 2006
- 19 percent of the survey participants could not identify the source of the spyware
- Of 57 percent that had banned IM in the workplace, 70 percent used obsolete, easy-to-defeat, or ignored methods to try and enforce the IM ban

 W32/Rbot-GFL is a spyware worm that spreads through IM and network shares. It can:


- Allow others to access the infected computer
- Steal data
- Download code from the Internet
- Degrade systems security
- Be installed within the registry
- Exploit systems and software vulnerabilities
- Help facilitate Denial of Service (DoS) attacks

Most IM solutions use a centralized infrastructure. Centralized servers must handle capabilities such as routing messages and authentication. Because of the expenses and resources required in building and maintaining these infrastructures, many organizations choose to use outside services such as AOL, Yahoo!, and Microsoft. Each of the IM services typically offers many features. The features offered change quickly, but Table 1 shows what was in place with commonly used IM services at the time this paper was written.

	AIM	Google Talk	ICQ	Jabber	MSN	Skype	Trillian	Yahoo!
Application Sharing					X			
Audio Chat	X	X	X		X	X	X	X
Encryption	X			X		X	X	
File Sharing	X							
File Transfer	X	X	X	X	X	X	X	X
Group Chat	X	X	X	X		X		X
Mobile Messages	X		X	X	X			X
Multi-Network							X	
Text Chat	X	X	X	X	X	X	X	X
Video Chat	X		X		X		X	X
VoIP	X		X	X		X		X
Web Services Integration	X		X		X		X	X
Whiteboard					X			

Figure 1: IM services and capabilities.

As you can see from the capabilities listed, each of these services brings with it many, and often unique, vulnerabilities that must be addressed to appropriately reduce the risks of using IM within a business enterprise. Business leaders must address those risks now; IM usage within organizations, both sanctioned use and use against policy requirements, is rapidly growing. The exploits for IM vulnerabilities have grown right along with the popularity of IM. The FaceTime Communications and Peapod study mentioned earlier revealed security incidents through IM types of networks were up 2200 percent in 2005 over 2004. These incidents often involve leakage of sensitive corporate information and PII. For example, IM worms can install programs on your enterprise systems that will copy usernames, passwords, credit card numbers, PayPal account details, and other financially useful data.

 The Heartworm worm tricks users into clicking a link to receive a virtual greeting card. When clicked, data-theft malware is downloaded and the worm propagates to the user's IM contacts. The interesting aspect of this worm is that it looks like a hoax. The goal is for the victims to believe that they are victims of a hoax, not an actual malware infection.

There are many risks related to data leakage; IM:

- Opens new holes within the network infrastructure through which information can easily and unknowingly leak out, creating privacy and intellectual property loss concerns.
- Creates invisible communications channels that typical information security measures do not address, making it difficult to comply with legal, regulatory, and contractual requirements and exposing the organization to breaches.
- Creates new paths into end-user computers and networks for the stealth distribution of malware such as viruses, worms, spyware, rootkits, and SpIM. Fighting these increasing malware outbreaks, and even just trying to protect against them, can drain business productivity and resources.



Spam over IM (SpIM) typically occurs through a link appearing to come from someone on your buddy list. If the link is clicked, malicious code can be installed on your computer.

Many business leaders direct the IT folks to just block IM. However, in most organizations, simply blocking IM is not an option:


- Every IM network provider has a unique set of IP addresses for client connections. The IP addresses often change without notice, so firewalls and proxies cannot apply blocking policies using the typical black list of IP addresses.
- IM clients use port crawling—the ability to exploit open ports on the firewall. Blocking specific ports for the particular IM application will not work.
- IM protocols are proprietary and constantly change to deliver new and enhanced features. Firewalls, proxies, and most other security technologies within enterprises do not evolve at this pace. Likewise, IT organizations cannot realistically be constantly updating protocol signatures on the firewall to prevent IM use.
- IM connections are synchronous. This is much different from asynchronous Web browsing and email traffic. Firewalls and proxies are not designed to inspect and analyze real-time communication traffic such as IM, so network performance can suffer when trying to configure them to prevent IM.
- In a very short time, large numbers of employees have embraced and become, from their perspective, dependent upon IM communications with business colleagues. Blocking IM will likely result in unhappy employees, many of whom will find ways to bypass the IM blocks, possibly causing more problems.

Instead of curtly declaring no IM use is allowed within the enterprise, business leaders must look at all the issues involved and make a decision that will work best to prevent critical information from being leaked through these pathways while supporting the business benefits IM may provide.

Consider Email Vulnerabilities

Email has been used within organizations for a comparatively long time. It can be very beneficial and support business. However, there are many inherent vulnerabilities with email that organizations must continue to diligently address:


- Email messages are vulnerable to unauthorized access through misconfigured mailservers and end user errors
- Email messages are vulnerable to modification by those intercepting them, and by recipients who make changes within them before forwarding them on
- Email messages are vulnerable to spoofing. Just because an email message looks like it came from someone does not mean it actually did come from the indicated sender
- Email systems are vulnerable to DoS attacks from error or from malicious intent
- Email messages can easily contain PII and other sensitive information that is unsecured and should not be sent outside the organization
- Email messages are vulnerable to user errors, such as incorrect addressing, misdirection, inappropriate forwarding, and the unreliability of the Internet

 The Internet cannot be considered 100% reliable. Just because you send an email message does not mean that it will reach the intended recipient; it could end up being misdirected to inappropriate recipients, or be sidetracked for a significant period of time within one of the relay points along the way.


There are many issues involved with using email for business. A few significant ones include:

- Legal issues, such as potential need for proof of origin, dispatch, and receipt
- Uncontrolled remote user and Internet access to email accounts
- Email sent between organizations by individual members of staff may lead to unauthorized exposure of confidential or sensitive information and a breach of confidentiality, leading to bad publicity and possibly legal action

History demonstrates that organizations are exposed to legal actions for inappropriate use or mistakes made with email.


 Business can be exposed to libel writs as a result of what an employee has written in an email message, even if it was written in jest and intended only for internal distribution.

Organizations must not only ensure the confidentiality of PII but also that confidential corporate information that could impact brand value and share prices is not leaked. U.S. Stock Exchange regulations must be observed, along with federal data protection laws such as the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA). Business leaders must continue to diligently address email vulnerabilities and ensure appropriate use to protect PII, business intellectual property, and the business from regulatory fines and costly legal actions.

 It is not possible to establish a 100% secure email system—there are too many protocols, evolving technologies, and unpredictable human factors. However, business leaders MUST evaluate the involved risks and establish email systems in ways to address and reduce the risks to a level acceptable to the business while being in compliance with legal and regulatory requirements.

Policies and Education Are Very Important

No organization can absolutely prevent unauthorized transfer of data through messaging solutions; trusted users with authorized capabilities will sometimes make mistakes, and some will make conscious decisions that will result in sensitive data leakage and subsequent incidents. The human element is the weakest in the information security equation. This makes the establishment and enforcement of clear and comprehensive policies, along with ongoing education and awareness, so very important.

 Personnel must be given ongoing training and awareness for messaging policies to make the policies effective.


Implement policies, procedures and standards

There are many policies, procedures, and standards that must be implemented for messaging use within the business environment. Incorporate the following into your policies and practices to specifically help prevent corporate information loss:

- Require encrypted channels for messaging. Doing so will mitigate packet-sniffing attacks and other man-in-the-middle attacks that unscrupulous third parties may try against you.
- Do not send PII within IM communications.
- Block outbound Direct Client Connection (DCC) to help prevent intentional or accidental leakage of files to third parties.
- Use security tools to hide the hostname/IP address from other messaging system users.
- Do not allow personal messages to be sent using the enterprise messaging systems.
- Use spam filters on all types of messaging systems.
- Require emails that must contain sensitive information and PII to be encrypted. Provide a transparent or easy-to-use encryption solution to help ensure employees do this.
- Monitor and log email use to help prevent sensitive information from leaving the enterprise. Check for PII and other sensitive data going out from the enterprise.
- Monitor and log IM use to help catch inappropriate access before intruders can get to sensitive data. Most of the popular IM systems provide the capability to log online conversations with other users. However, this information is stored in a text file on the local workstation. A malicious user who has access to this workstation can retrieve this file and have access to all information that was exchanged during an online conversation. Be sure to implement messaging logging in a centralized location.

Awareness and Training

When you have your policies, procedures, and standards established, you must communicate them to personnel; not only once but also through periodic training and ongoing awareness messages. More reports of incidents occurring through mistakes or malicious actions appear all the time. You must educate the individuals using your messaging systems about how to use them correctly to help prevent sensitive business information and PII from being leaked out to criminals, competitors, and the general public.

 You cannot expect personnel to use messaging systems appropriately and successfully protect PII and other sensitive information if you do not tell them, often and in many ways, what appropriate use is and how to secure related information.

Include the following topics and communicate the associated messages—tailored for your business environment—within your awareness and training efforts to specifically address the prevention of data leakage through messaging systems.

Social Engineering

Social engineering is pervasive on IM services. Buddy lists allow users to add contacts that they are familiar with to their lists. The assumption is that if someone contacts you, they have received your name from a friend, when in fact it could have been gained through a simple dictionary attack. Beware of social engineering attempts.

Identity Theft

Identity theft can occur in many ways and puts you and the business at risk. For example, by posing as an employee of an IM service, a malicious user can trick someone into giving information such as usernames, passwords, and credit card information. This information can be used to compromise other systems and services and can lead to theft. Another method of identity theft involves obtaining usernames or passwords through decryption on the local workstation or through a packet capture utility. Programs such as dsniff are able to decrypt passwords for some IM services over a network on the fly. Other utilities, such as Cain and Able, can monitor network activity and decrypt passwords.

File Transfers and Messages Spread Malicious Software

One of the most dangerous security risks for IM and email is the ease with which Trojans, viruses, and other malicious code can be spread. IM in particular is vulnerable to these threats through the file transfer feature. Sending files in this manner creates a direct connection between users, bypassing the centralized network scanning used to provide malware protection. Once these pieces of malware infect a machine, they can spread to other machines, creating massive amounts of network traffic and overloading a network. Depending upon the configuration of IM, it is possible for files to be transferred without your knowledge. This could allow sensitive information to be transferred from your workstation, or a file you have access to on the network, without your permission.

Worms and File Transfer Through IM Get Around Enterprise Security Devices

Worms are capable of spreading over IM and typically appear as a uniform resource locator (URL). These messages will usually come from what appears to be someone on your buddy list, so it is more likely that you will click them. Once clicked, the worm will infect your computer and spread to everyone on your buddy list. Some worms and viruses that spread via IM send an infected file to users and are able to avoid being detected by the network antivirus system. Do not click URLs if you did not expect to receive one, even if it looks like it came from one of your buddies.

IP Address of Workstation May Be Revealed

Some IM features, including file transfers, reveal the IP address of the workstation being used. This can allow for unauthorized access and capture of sensitive files and PII on your computer and the enterprise network.

Encrypt Messages and Files

When communicating sensitive information, such as PII and company intellectual property, encrypt your messages and any files attached to them. This applies not only to email but also to IM. And never discuss sensitive information over IM unless the conversation is encrypted and you know for sure who the buddy is you are communicating with.

Watch out for SpIM and Offensive Material

SpIM is becoming quite common and is carried out by automated bots to collect data from IM users' systems. For example, they can copy IM names and send marketing messages to those users. SpIM typically contains URL links that go to sites with malicious code, pornographic material, or other inappropriate or dangerous sites. Do not click on URLs within your IM messages to help prevent being a victim of SpIM. Help prevent unwanted SpIM messages by changing the settings in your IM client to ignore messages from unknown users.

Follow Email and IM Compliance

Know and follow the company's email, IM, and other messaging policies and requirements. If you do not, you will not only put yourself and your job at risk, you can also put the business at risk along with the PII of customers and your fellow coworkers.

Don't Trust Unsolicited Instant Messages

If you receive a suspicious IM, such as a message containing only a URL link with a brief or vague phrase from a friend, verify that your friend, and not an IM bot or virus, sent you the link. Do this by typing something back to the person who sent it asking something such as, "What is this? Why should I go there?" If no one responds, it is likely a bot sent it.

Use BCC Within Email Messages

When you send a message to a group of people, consider putting their email addresses within the blind carbon copy (BCC) field. Definitely do this if the members of the group are from different organizations or do not know each other. Not only would putting a large number of email addresses in clear text in the TO field leave the message open for spammers to harvest email addresses, it also protects the privacy of the people to whom you are sending the message. You should not provide someone's email address to others, particularly strangers, without permission.

Be Very Careful When Forwarding Attachments and Email Messages

Except in a work environment where it might be expected within your internal network, check with your intended recipient before sending attachments. If it is a large file, consider that sending it may block their account from receiving additional email because they exceeded their disk space quota. You need to avoid inadvertently sending a file with PII or other sensitive company information that your recipient should not have.

Be Very Careful When Opening Attachments

Use great care when opening email and IM attachments, even if they appear to come from someone you know. If you receive an attachment that you are not expecting, don't open it. First read the message and make sure that the attachment is most likely legitimate. If you're still not sure, get in touch with the sender to be sure. If the sender's computer has a virus, it may be attaching trojans to all outgoing emails from them. If you're opening spam, it could direct floods of it to your inbox, multiplying the time you're chained to email by an order of magnitude. Web bugs (one pixel GIFs) may be embedded and could send a signal back to a remote system, sending sensitive information from your computer or the network to fraudsters and criminals.

Be Careful

Remember that email and IMs can be intercepted anywhere en route to the recipient. Remember that these messages could exist for years in recipient email boxes, later coming back to haunt you with inappropriate information or sensitive information you sent. Stop and think before sending email you will later regret.

Use 'Reply All' With Care

Do not use "reply all" if other recipients of a group email do not need your response. There may be information you are replying with that all recipients should not receive. You may be inadvertently sending sensitive information outside the organization by using "Reply All."

Proofread Your Messages Carefully

Proofread your messages carefully before sending them. Make sure you are not sending information that should not be going out to your recipients. Make sure you have the correct recipient email addresses and have not accidentally included an address for someone who should not receive your message. Make sure you have removed sensitive information if you are forwarding another message that you received.

Don't Unsubscribe Blindly

If you start receiving “subscription” emails from some source to which you did not subscribe, do not use their “unsubscribe” link. If you do, you might just find yourself getting even more emails. You’re better off just adding the email address (or the entire domain) to your inbox blacklist.

Don't Be Hooked

Phishing messages, such as those commonly claiming to be Paypal, Western Union, eBay, numerous banks, and many other organizations, typically indicate account closure and balance forfeiture if you do not click on included URL links to “verify” your account details, or they warn you that your account has been compromised and that you must click the URL link provided to address the “serious” situation. The URL links look legitimate but will instead direct you to a lookalike site set up to collect your login and password information, credit card, and/or bank account details, and so on. Never click links in these types of messages. Honest companies never send this sort of email; they will never send an email where they tell you to click on an enclosed URL link to save your account from shut down or to verify your ID and password.

Implement Messaging Security in Depth

The most effective way to reduce the inherent risks associated with messaging is to implement a combination of technical protections along with effective management strategies and policies and ongoing awareness and training.

Article 5: Addressing Image Spam

What Is Image Spam?


Have you noticed an increasingly large number of email messages coming into your inbox that have the text information imbedded within graphic images? Some of the most common types are those represented in Figure 1.



Figure 1.

Another common image spam is one giving "hot stock tips." After the recipients bid up the price of the listed OTC stocks, the spammers then dump the stocks for a considerable profit.

The text portion of image spam frequently contains meaningless quotes from literature or copies of the latest news headlines, along with animated, tiled, oddly colored, and/or layered graphics that divide the message into multiple images stacked on top of each other. Many have even removed the typical links to click and instead direct the message recipient to type the URL into the browser; they do this because most filters look for the known malicious, clickable URLs within the email message.

 According to Secure Computing research, the amount of spam has tripled throughout 2006, with a further 50% increase in just the first couple of months in 2007. Their research also indicates that spam now accounts for nearly 90% of all email, of which 30% is image spam.


Marshal's Threat Research and Content Engineering (TRACE) 2006 Report that was released on March 5, 2007 reported "Image spam normally accounts for 15 to 20 percent of all email but right now is accounting for more than 35 percent."

F-Secure indicates that "Image spam is taking up 70% of the bandwidth bulge on account of the large file sizes every single one represents."


Why has image spam become so popular? Because it is sneaky and effective for the spammers. Image spam defeats most spam filters. The clever spammers are fooling most spam filters by putting graphical text within an image so that the system doing the filtering just sees code, not the letters and numbers the recipient sees within the graphic.

Image Spam Negatively Impacts Business


Image spam can not only cause huge headaches to the IT folks but also bring a business to a halt if not addressed. Image spam is much more difficult to detect with conventional content analysis spam filters, is usually much larger than text-based spam, and takes significantly more bandwidth and storage. Image spam can flood your network and bring it to a standstill. If you depend upon your network for business processing, you could find yourself dealing with a non-responsive, spam-flooded network, with no access to your business applications or customers.

 Businesses that rely upon their network for business success must address image spam and its negative impacts or suffer negative business impacts.

More sophisticated spam filters have tried to identify the letters inside graphics using optical character recognition (OCR) technology. However, the spammers have gotten wise to this and now have methods for outsmarting OCR. For example, they will use unusual fonts or put a lot of additional information and images, such as added color, gaps in letters, and so on, within the graphic so that the OCR does not recognize the letters.


 Very generally, “botnet” refers to a collection of software robots, zombies, or bots that run on their own. Botnet can also be used to reference a network of computers using distributed computing software, typically some type of malware.

Another problem is that image spam and botnets are being used together. Botnets are what propagate most spam, but now botnets are also being used to alter a spam message image by changing the size, shape, colors, and so on so that it looks different to the filters that sort out identical emails.

 As of October 2006, Secure Computing research identifies an average of more than 250,000 new zombie, or botnet, machines *every day*—an increase of 50% from only a few months earlier.


Addressing Image Spam Threats

Businesses must address the image spam problem to keep it from bringing their business processes to a grinding halt.

-  A few of the challenges for fighting image spam
- Multiple email servers and network entry points
 - Overloaded email servers with outdated tools and monitoring
 - Inadequate quality of email service

Some of the ways in which image spam can be addressed include:

- Use a single email server with a single entry point. Limit the ways in which image spam makes it into your network. Make sure all messages are scanned before they have a chance to negatively impact your network. Don’t allow email messages to be accessed through Web-based mail systems.
- Use tools that analyze sender reputation. Is the sender known to have sent spam in the past? When was this sender seen for the first time? How much email is this sender responsible for? Does the sender both send and receive email, or only send emails? Is the sender’s behavior sporadic or continuous? Is the sender on blacklists?

 Sharp increases in sending behavior as opposed to a regular amount of inbound and outbound email, is one indicator of spamming. Senders who have an unusually high ratio of sent mail to received mail often are discovered to be spammers.

-
- Check the message reputation and fingerprinting. Does the message contain parts of previously received spam? Does a comparison of the image contained in the message contain similarities to known spam images? What are the network characteristics involved with the delivery of the message?
 - Invest in effective, forward-looking technology. Vendors are working all the time to improve spam filtering, and image spam filtering in particular. It is not possible for your email administrators to keep out image spam using old methods.
 - Review and update your email policy. If image spam is causing you particular problems or having a noticeable negative impact on network performance, consider blocking all attachments on incoming email. If this is not feasible, consider routing emails with attachments through a quarantine area for review first or allow only certain departments or groups to receive email with attachments if that is common for your business purposes.
 - Keep your email systems updated. Image spam exploits vulnerabilities in unpatched email servers.
 - Educate your personnel. First make sure they know the characteristics of what image spam looks like, then tell them to never reply to those odd-looking email messages, and not to click the links within them.
 - Use your corporate lobbyists to strengthen government laws and industry policies. Make the penalties and fines for spamming more severe to help motivate these spammers not to continue with their disruptive messages. Doing so will also help keep marketers from trying to use image spam, as they are using it more because their other types of mass marketing messages are caught by the spam filters.



An interesting site with information about a wide range of spam types is the Spammer's Compendium (<http://www.jgc.org/tsc/>). It contains useful analysis for specific image spam messages.

Article 6: What Businesses Need to Know About Reputation-Based Messaging Technology

An Overview of Messaging Filtering

Email security and annoyances have been plaguing organizations since email left the mainframe and dumb-terminal-only view and started residing on distributed mail servers, communicating with anyone who wants to send messages from outside the enterprise network. One of the first types of malicious and annoying email messages that started to occur was spamming. It was soon followed by fraud schemes, then phishing. Security has been trying to keep up with all the new and clever ways to get around the protections that organizations implement to try and keep spam and related types of malicious messages from entering the enterprise network.

Some messaging filtering methods work better than others. Some worked fantastically well when first introduced, but then the evolution of spamming methods soon outdated the once wonderful spam fighter. When new message-filtering solutions are rolled out, the spammers adjust their spam delivery methods to defeat the filters. What messaging security methods have been used? Table 1 provides a brief overview.

Security Method	Description
Blacklist	A blacklist is a list of email addresses and Internet domains that identify that specific mailservers originate spam and so should disallow or delete all corresponding messages without any further analysis. Basically, if a sender or sender domain is on the blacklist, it is considered spam.
Whitelist	A whitelist is a list of email addresses or Internet domains from which messages will always be accepted. Anything not on the list is always rejected.
Content filtering	Filtering technologies compares the From field, and/or the Subject field, and/or the message body with a list of words or Internet domains known to be used by spammers. If there are matches from known spammers and spam messages, the domain and/or sender is put in the email client's blacklist and the filter then treats it as spam from that point forward.
Bayesian filtering	Generally, this technology allows a spam filter to "learn" the characteristics of spam using a statistical analysis of message length and the distribution of words present in a message. Messages are put through a Bayesian filter many times, and the administrator tunes it to determine what is spam and what is not to a typical 90 to 95% accuracy rate.

Security Method	Description
Heuristic detection	Heuristic analysis uses a rule-based approach to determining whether an email message is spam by using a type of analyzer engine. The engine works through a rule base, checking the message against criteria that indicates possible spam. It assigns points when it locates a match. If the total point score meets or exceeds a specified threshold score, the file is flagged as suspicious and processed accordingly.
Mail retrieval proxy	These programs insert themselves between the email client and the mail server from which the email is delivered. All the email passes through the mail retrieval proxy, which then filters for spam and either deletes the spam or marks it so that the email client can delete it after being inspected by the recipient.

Table 1: Messaging security methods.

There are problems with these typical types of filtering. One significant problem is with misclassification of the messages. Messages are often misclassified by:

- Flagging legitimate email as spam; a “false positive”
- Flagging spam as legitimate email; a “false negative”

These misclassifications have a significant cost to organizations. False negatives use valuable bandwidth and storage and degrade overall workforce productivity. False positives can result in lost business that results from lost orders and communications and perceived unresponsiveness. Newer and better methods for filtering were needed.

What Is Reputation-Based Technology?

In December 2005, the U.S. Federal Trade Commission (FTC) published “Effectiveness and Enforcement of the CAN-SPAM Act: A Report to Congress,” indicating spam has become more targeted and clever in the methods used to bypass the traditional filters. In the past few years, reputation-based technologies have emerged to improve upon message-filtering success.

Application of reputation technology is very similar to establishing credit scores at a bank. At a very high level, the local spam defense appliance creates a profile of all message sender activity on the Internet and then uses the profile to watch for deviations from expected behavior. The system uses global trusted sources in combination with knowledge about the enterprise to generate a reputation score based upon the behavior of the sending host. This score is then used to determine whether messages are good, are confirmed spam, or are suspicious.



Some of the techniques incorporated into reputation-based technologies include:

- Anomaly detection
- Blacklists
- Bulk-mailing detection
- Content analysis
- Forgery detection
- Header analysis
- Malicious URL detection
- Spam honeypots
- Spam signatures
- User-reported spam
- Whitelists

Reputation-based technologies can broaden the context in which the message is evaluated, improving catch rate and accuracy. For example, effective reputation-based technologies can defend against the use of embedded URLs by reviewing multiple parameters to evaluate the reputation of the associated Web sites.



[Http://www.TrustedSource.org](http://www.TrustedSource.org) is a very interesting site that allows anyone to check current and historical reputation and sending patterns of email senders as well as view analytical information such as country of origin, network ownership, and hosts for known senders within each domain. This site also shows global email and spam trends.

Features to Look for in a Reputation-Based Spam Filtering Solution

Be sure to check the capabilities of a reputation-based spam filtering solution before investing in one. To be most effective, a reputation-based solution should:

- Measure the behavior and traffic patterns of a Web site to assess its trustworthiness; this will provide improved protection against spam, viruses, phishing, and spyware threats
- Use as large a volume of reputation data as is possible
- Use high-quality reputation data; reputations should be correlated by most effectively aggregating global behavioral and pattern knowledge data
- Use highly accurate reputation data; without high accuracy, organizations will experience high numbers of misclassifications
- Integrate and correlate multiple signature- and content-based detection techniques; these multiple layers create a much richer and comprehensive knowledge database and will help to minimize the risks of misclassifications
- Allow for real-time updates to the knowledge base to provide the ability to stop as many brand new (zero-day) threats as possible before they can enter the enterprise network
- Block emails from known spam sources
- Block directory harvest attacks and bounced mail attacks
- Detect image spam
- Apply embedded URL reputation data to block emails with links to malicious Web sites

Article 7: Security Products Must Be Secure

Software Vulnerabilities in the Security Products Industry


Every week, it seems there are headlines about security products containing vulnerabilities that put the organizations using them at risk. For example, consider the following examples from the March 15, 2007 issue of Virus Bulletin (available at http://www.virusbtn.com/news/virus_news/2007/03_15.xml):

- “Several vulnerabilities have been found in McAfee’s ePolicy Orchestrator management tool, which could be exploited to gain remote access to systems running the software. Patches have been made available and users are advised to ensure they are applied as soon as possible. Several versions of EPO 3, as well as ProtectionPilot, are thought to be affected.”
- “Trend Micro, already hit by a string of vulnerabilities in recent weeks, has suffered another problem in its antivirus engine, which could cause a full system crash on exposure to a carefully crafted malicious file. The problem, caused by a divide-by-zero error in processing UPX compressed files, affects version 8 of the Trend engine, and while some systems may only lose service from the malware scanner, Windows users could suffer a ‘Blue Screen of Death’ (BSOD) crash of the whole operating system.”

The vulnerabilities are not found just within antivirus software. Because of the complexities involved with networks and the rapidly increasing types of technologies deployed, no computer system that is useful can be completely secure. And likewise, no computer system security product can ever be guaranteed to be 100% secure. However, business leaders must still perform due diligence when choosing a security product to ensure that everything possible has been done by the vendor to remove all known vulnerabilities, and that the vendor will continue to diligently update their product to ensure all newly discovered security flaws are quickly and effectively removed.

It is of utmost importance to implement secure networks and applications. An ongoing barrage of electronic attacks on computer systems, along with an ever-increasing multitude of threats to end-user computers requires the use of information security products. Unfortunately, many vulnerabilities are also found within the very security products purchased to protect the enterprise.

It is common for organizations to perceive an immediate need to close a vulnerability or obtain compliance by purchasing additional security hardware or software products. Often the product purchase decision is then based upon the best-sounding sales claim, what is most readily available, suggestions from colleagues, or what best fits the budget. Often in-depth review of the security product gets overlooked. Third-party independent evaluation of the product is probably the best indicator of the product’s effectiveness, but oftentimes this is not available or, when it is, the depth of review of the product is not deep enough to hit the full scope of security concerns or does not cover issues unique to your organization.

-
-  A highly trusted security system yesterday may be reduced to an untrusted security system tomorrow through many means:
- A previously undiscovered vulnerability in a specific operating system (OS) or other application is announced
 - An update to the software configuration is installed with flawed code
 - A lapse in security procedures within the vendor occurs due to a change in key personnel
 - The vendor is acquired by another company and support for the product is either discontinued or drastically reduced

It is important to keep in mind that just because a security product used to be secure does not mean it will always be secure. Individual parts of a security architecture and a system's past performance are not always indicators of future trust performance characteristics.

Costs Associated with Vulnerable Security Products

Many threats against data and resources can exist when security products contain vulnerabilities; for example:

- Bugs in operating systems and application software can create exploitable vulnerabilities
- The software may not be robust enough to prevent errors made by end users and administrators
- Programmers may forget to remove backdoors to the software before launching into production
- Disgruntled employees may make changes that create vulnerabilities that they can then exploit

What are the problems associated with implementing a substandard or buggy security product? They can be substantial:

- Inability to access critical business processes on the network for prolonged periods
- Loss of an e-commerce Web site for hours, days, or weeks
- Damaged, lost, or stolen data
- Noncompliance with applicable laws and regulations
- Civil actions resulting from privacy breaches
- And many more...

Hardened Security Software Is Necessary to Protect Business

Organizations must ensure that the security products they implement are secure. Just as you expect that the brakes have been validated to work appropriately in your new car, and that your home security system has been tested to consistently set off the alarm when an intruder tries to break in, you must also use network and computer security products that do not have any security vulnerabilities. If you do not, the security products themselves will put your business at risk.

Before making a security product investment, be sure to confirm the product is as free of security bugs as possible. By doing so, you will protect your business by:

- Providing a baseline level of security to protect your enterprise from common and dangerous local and remote threats
- Ensuring a consistent approach to securing the systems upon which your business depends
- Significantly reducing the valuable time required to perform maintenance on security products
- Preventing embarrassment or public loss of confidence due to compromise of publicly accessible systems that resulted from vulnerable security products

Examples of Security Products that Must Be Hardened

It is critical—due to the purpose and nature of the product—that security tools and solutions are hardened as much as possible.



Commercial-Off-The-Shelf (COTS) product evaluations are conducted through the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS). The NIAP is jointly managed by the National Institute of Standards and Technology (NIST) and NSA and staffed by personnel from those agencies. For more information, see <http://www.nsa.gov/ia/industry/niap.cfm>.

The types of security products you need to ensure have hardened security include:


- Application frameworks
- Application servers
- Antivirus software
- Automation/productivity application suites
- Database Systems
- DHCP servers
- Directory services
- DNS servers
- Firewalls
- Email servers
- Multi-functional peripherals
- Network routers
- Network switches
- Operating systems (OSs)
- Vulnerability management software
- Web browsers
- Web servers
- Wireless networks

25 Questions to Ask Security Product Vendors


NIST, with sponsorship from the Department of Homeland Security (DHS), has produced the *Security Configuration Checklists Program for IT Products: Guidance for Checklist Users and Developers* (available at http://checklists.nist.gov/docs/SP_800-70_20050526.pdf) to facilitate the development and dissemination of security configuration checklists so that organizations and individual users can better secure their IT products. This document is useful and rich in detail and insights. It not only breaks down the security issues that organizations must consider when choosing a software product but also discusses the issues vendors should be addressing when creating the products. It is a great document for your IT development and implementation team to use.

The following high-level quick-use checklist incorporates some of the NIST security hardening requirements as well as leading practices and my own experiences with helping organizations choose a hardened security product. Use it to help with your security product evaluation process and to facilitate discussion with your development and implementation teams.

- 1. Are the default security settings consistent with recommended practices?** It is common for some vendors to set their security settings at the least restrictive levels instead of at the level that is most secure for the majority of organizations.
- 2. Could any of the security product settings cause the product to become inoperable or unstable?** New features that have not been thoroughly tested could cause the product to fail when configured certain ways.
- 3. Do certain settings reduce product functionality? If so, is this documented?** Sometimes security features have been engineered in ways that cause bandwidth or storage problems, resulting in making the product virtually non-functional within enterprise networks.
- 4. Do the security settings take into account recent vulnerabilities?** Security products should be updated as soon as possible to address new exploits.
- 5. Did independent third parties conduct security assessments on the security product?** Third-party security assessments are increasingly showing up in requests for proposals (RFPs) and service level agreements (SLAs) for packaged and on-demand software.

 The term *on-demand software* generally describes software delivered to the customer via a network (such as the Internet) as a service.

- 6. Has the security product been independently evaluated using the Common Criteria (CC)? If so, at what evaluation assurance level (EAL)?** Under the CC, different classes of products are evaluated against the security functional and assurance requirements of “protection profiles.” Protection profiles have been developed to apply to OSs, firewalls, smart cards, and other products that can be expected to meet security requirements. The CC specifies a series of EALs for evaluated products. A higher EAL certification specifies a higher level of confidence that a product’s security functions will be performed correctly and effectively.

 For more information about the CC, see <http://www.niap-ccevs.org/cc-scheme/>.

- 7. Does the security product vendor disclose all vulnerabilities that exist within the software?** Some vendors only disclose vulnerabilities after a patch is ready and posted on the same day as the disclosure, even though they knew about the vulnerability long before that.
- 8. What technical guidance does the security software vendor provide about vulnerabilities, including how they could be exploited, how they are currently being exploited, and how to mitigate?** Software vendors that practice customer or public vulnerability disclosure are generally diligent about explaining their mitigation strategies.


-
9. **Does the security product vendor have a dedicated team to assess and respond to security vulnerabilities reported for their products?** Because most software vendors have a way to report and respond to bugs, security defects should be easily added to this process.
 10. **Are reported security defects treated differently than non-security defects?** You want to make sure security defects within security products are elevated to a higher priority fix.
 11. **Does the security software vendor have staff to simulate security attacks against the product prior to release?** Most vendors still lack the internal expertise to dedicate staff to security-specific testing.
 12. **Does the security software vendor provide severity ratings for vulnerabilities, and how they are determined?** Some companies are good at defining and sharing their severity rating system. You must understand, however, that severity is a subjective measure, so you will need to determine for yourself how severe a vulnerability is for your environment.
 13. **Is security reviewed at each phase of the software development life cycle (SDLC)?** Very few companies have incorporated security within all phases of the SDLC even though this is the most effective way to ensure security works as necessary and intended.
 14. **Does the security software vendor use automated tools for security testing or code review?** The use of automated tools to test security is increasing, but be sure the engineers using it are trained; there is no value in a tool that is not used correctly.
 15. **Has the security software vendor created the software to ensure ease of use? What tests were performed to accomplish this? Did they use independent test groups to validate ease of use?** Even the most technically effective security product will be diminished in value if it is difficult for your personnel to use.
 16. **Does the security software vendor monitor the latest attack trends in the underground community and consider how those trends may affect their software?** Vendors that are proactive with security disclosure and severity ratings typically conduct these types of activities.
 17. **What are the terms of the security software vendor support agreement? Will it ensure that all critical security defects will be fixed quickly, such as within 1 month of discovery?** Few vendors will make such a statement or commit to it contractually. However, the more customers ask for such terms, the more vendors will feel pressured to quickly address security vulnerabilities.
 18. **Has the security software vendor ever released an emergency security patch?** This will help point to the responsiveness of the security vendor.
 19. **What is the security software vendor's patch release strategy and what tools do they offer for patch deployment?** Many, if not most, vendors do not provide regularly scheduled releases, and few offer fully tested patches. You often do not get both timeliness of a patch and a fully tested patch. You may need to decide which is most important for your organization, timeliness or fully vetted patches.

-
- 20. What methodologies does the security software vendor use for security testing their products?** Look for methodologies adopted from NIST or based upon frameworks and standards such as COBIT, the CC, or ISO 27001.
 - 21. What methods does the security software vendor use to inform customers of vulnerabilities?** Registered customers should have vulnerability information disclosed to them immediately, even before the associated patch is ready. It is also good if the vendor allows you to choose the method of disclosure, such as by email or phone. Be aware that many vendors believe that no disclosure at all is the best policy, or they choose just to notify their customers and the public only after a patch is ready.
 - 22. What percentage of the security software vendor software development and testing team is focused on security?** A security product vendor should have staff dedicated solely to security. Look for a vendor that has personnel doing testing for all the different aspects of software quality (functionality, reliability, performance, usability, accessibility).
 - 23. What training does the security software vendor development and testing team receive specific to application and systems security?** They should put all their personnel through some type of security training, and they should provide ongoing awareness. Unfortunately, many software vendors still do not provide adequate security training and awareness to their own personnel.
 - 24. Is the security product compatible with your legacy systems?** Organizations often purchase security products only to find upon installation that the products are incompatible with the organization's existing security software.
 - 25. Does the security vendor have substantiated testimonials to provide from other customers who use the product? Is contact information provided so that you can contact the other customers to ask about their experiences and satisfaction with the product?** It is good to confirm from others actually using the software that it does indeed work as promised.

Article 8: Reducing Attack Exposure for Internet-Facing Applications

Build In Security

The more software you have and the more options that are available for client machines to communicate with your software, the less secure your networks and data.

 Increasing complexity increases vulnerabilities.

If you have just one non-secured application, you open a potential attack path that may be exploited, circumventing all the other security you've implemented on your other servers and possibly allowing a nice little pathway through your firewall via that application vulnerability in ways that other direct attacks upon the firewall would fail. Figure 1 shows how, with even the strongest firewalls and applications, just the existence of one application could allow an attacker to wreak havoc throughout your network and your organization by shutting down access to the systems upon which you depend to conduct business.

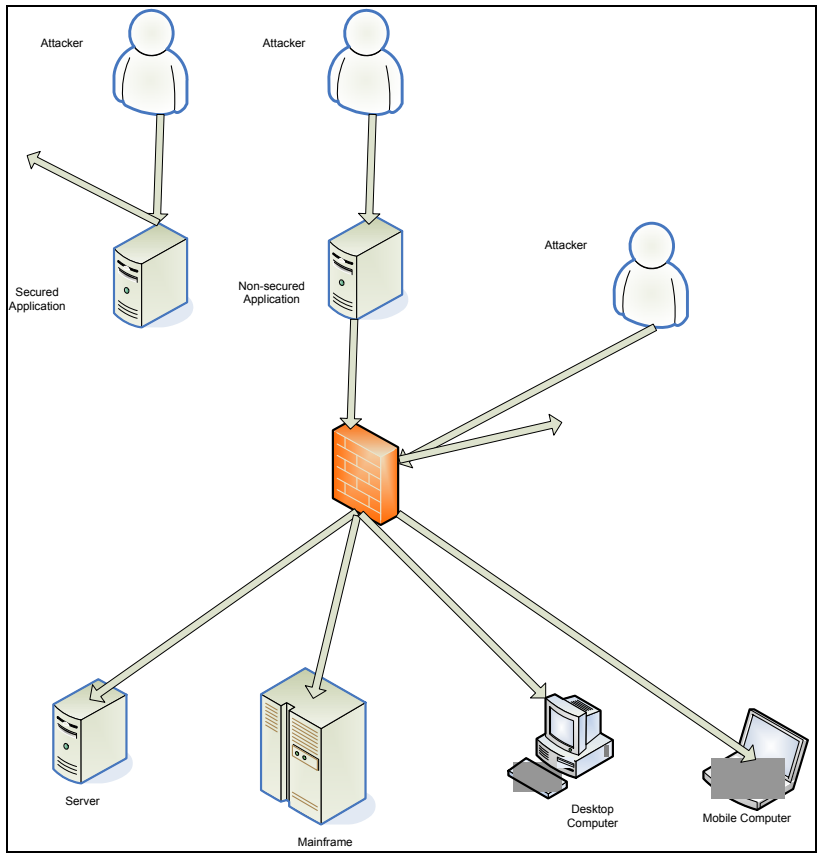


Figure 1: Attack paths through one application vulnerability.

Applications security is fundamentally a software engineering problem. It must be addressed in a systematic way throughout the entire software development life cycle. During this process, the software engineers and developers must minimize access to data and network resources using built-in granular controls to maximize application security.

Attack Methods

Lack of thorough and thoughtful security engineering can leave many vulnerabilities within an application. A small sample of attacks that exploit application vulnerabilities include:

Type of attack	Specific exploit
Denial of Service Attacks	Invalid packet lengths
	Flooding with random MAC addresses
	Malformed packet headers
Spoofing Attacks	Spoofing Internet headers
	Invalid Source IP with correct ports
	Race condition responses
Firewall Rule Set Bypass Attacks	Random UDP data to bypass rules
	Port scanning detection
	Connection prediction
Exploit	Send mail Header Overflow
	WFTPD Overflow
	Wu-IMAPD Overflow
Brute Force	Massive GET/POST requests
	Anomaly detection
Hijacking Sessions	XSS redirection (UNICODE)
Directory Transversal	Try “..” and other traversal methods
	UNICODE traversal methods
	Mixed strings


The most fundamental security action to help protect the enterprise from Internet-based attacks is to design your Internet-facing application to disable all capabilities not relevant to your organization’s use of the application. Another important defense not utilized nearly enough is to disallow all types of access by default and allow only those necessary based upon roles.

Positive Security Models vs. Negative Security Models

There are generally two methods currently used to defend against all types of application server attacks; the negative security model and the positive security model.

Negative Security Model


The typical method used by most security products and organizations is the negative security model. This approach basically identifies and disallows the specific types of traffic and access attempts already known to be threatening while allowing all other requests and access attempts. Antivirus and intrusion detection and prevention systems are classic examples of this approach. They both check requests and traffic flows against attack signatures. This type of approach used to work fairly well. However, new threats are emerging more frequently than ever before, and their number will continue to increase. This will result in considerably less time on an ongoing basis to react to the steadily increasing new attacks over time.

 A negative security model tries to figure out if there is something dangerous in the traffic. Negative security models are easy to start working with but you cannot create a foolproof rule set. Negative security rules are written only for known problems, exploits, and Web application attacks.


Positive Security Model

The positive security model denies all types of access and allows only those specific access capabilities to specific roles based upon authorizations. For example, consider the dozens of application-specific proxies that exist, such as application filtering for email, Citrix, Oracle, SQL, VoIP, Web, and other commonly used Internet protocols. When the positive security model is used, each proxy is configured according to your organization's unique use of the applications. This configuration then becomes the standard against which all traffic trying to use the application is checked.


Application-specific filters enable organizations to define very explicitly how the applications can be used based upon group rules. The firewall can then allow very granularly only those access capabilities based upon only the permitted use of these group rules. Such granular role-based group access controls help to ensure that suspicious traffic that does not conform to your corporate rules can be filtered and prevented from entering your enterprise, even for zero-day threats.

 Organizations need to establish granular role-based group access based upon the business' information security policies, business group responsibilities, leading industry practices, and RFC compliance.

The positive security model approach allows only legitimate, acceptable traffic elements and denies everything else.

 The positive security model tries to ensure the incoming data is safe to use, and that the incoming requests are safe. This is a much more effective goal than allowing all traffic and trying to detect all the bad stuff.

The positive security model is based upon sound security practices that have existed for decades, but were somehow lost along the way within most security product development efforts. A positive security model mirrors business application logic. So, whenever the application changes, the security model must be updated. For example, if you have an application variable such as “account” that will be all numerals, then you should have a rule defined that will check and ensure that the contents of “account” are all numerals or they will be disallowed. If your “account” changes to be all alphabetic, then you will also need to change your check to allow only all alphabetic “account” values to be allowed. This example is very simplistic, but it demonstrates the common sense approach of the positive security model.

 Although more secure, the positive security model is also more difficult to deploy because it needs to be custom configured to the specific application being protected.

Providing Granular Access to Applications

The positive security model utilizes granular access controls to application capabilities. Access controls can be made on a very specific level to any user, program, or process that requests permission to data or tries to perform specific business process activities. The access control subject (for example, the user ID), the access control object (for example, a specific database), or a combination of the two can define the access control authorizations.

The access control subject can be based upon:

- The time of day or day of request
- The location from where the access control subject authenticated
- Password or token utilized
- And so on

An individual access control subject may have different rights assigned to specific passwords that are used during the authentication process

The access control object can be based upon:

- Classification of the data content of the object
- Transaction restrictions
- And so on

The access control subject may be restricted from accessing all or part of the data within the access control object because of the type of data that may be contained within the object

The attributes of a subject are often referred to as privilege attributes or sensitivities. When these attributes are matched against the control attributes of an object, the privilege is either granted or denied.



Assign Access Privileges to Subjects Using Roles

The configuration of privileges in access control for an individual subject or user provides the most granularity. However, in enterprises with hundreds or thousands or more users, assigning and maintaining the granularity becomes a huge management burden. By giving multiple subjects similar permissions based upon their business roles, such as job titles or department teams, this granularity can still be achieved with more simplified access control administration.


Configure Access Privileges to Objects Using Roles

The configuration of privileges to access an individual object provides maximum granularity. It is not uncommon today for the number of objects within an access control system to number in the tens or even hundreds of thousands. Although configuring access to individual objects results in the maximum control, this granularity can quickly become an enormous administration burden.

It is a common practice to assign the appropriate permissions to a directory, then each object within the directory will inherit the respective parent directory permissions. By incorporating multiple objects with similar permissions or restrictions within a group or directory, the granularity is maintained but the administration of the access control system is simplified.

-  Stateful inspection firewalls only open and close ports; they are not role-based. Leaving ports wide open or completely closed does not provide for role-based granular access controls.
-  Network-layer firewalls have little awareness of the applications they are supposed to be protecting, so their connection controls cannot be granularly customized to each client's unique use of their own applications.

By implementing application access in granular ways, organizations can improve security and better monitor traffic. This can be achieved through the use of application-layer proxies. Granular access controls through the application's connections can allow for different roles to be given different types of access.

-  Implementing application-layer proxies significantly increases security. Stateful inspection firewalls only open and close ports.

Restricting Applications Capabilities

The concept of using granular access controls can also be used to restrict the capabilities of applications that will result in improved security. For example, you can restrict access to Internet-facing applications by screening all access requests through a tightly configured application gateway. By restricting application access in a granular method based upon roles, you can also prevent sensitive data leakage.

Firewall type	Characteristics
Application layer proxy	<ul style="list-style-type: none">• Communicates directly with the untrusted Internet requester to determine whether or not to allow the access through to the application server.• The only way an attack is going to get through to the internal application server is if there is an error in the proxy's logic, or the attacker invents a new attack that fits within the proxy's idea of 'acceptable traffic' for that protocol.
Network layer	<ul style="list-style-type: none">• Allows untrusted requestors to have a direct packet flow to the internal application server if the port is open.• Once the source/destination/origin has been deemed acceptable, the external client traffic is allowed straight through, unmodified, and passed directly to the internal system behind the firewall.

A major problem with application-layer proxies is that they are considered too slow. To address this issue, it is effective to remove the applications capabilities that you don't need so that the application-layer proxy does not need to spend more time checking those capabilities. This not only speeds the access request processing but also helps to prevent data leakage through capabilities you don't really need.

Get Rid of What You Don't Need

For example, what if you do not need to allow application users access to databases for some specific predefined storage procedures? Most organizations leave those capabilities intact. However, if you do not limit the access appropriately, this leaves the risk that an attacker could do something bad through that capability, such as mounting an SQL injection attack to retrieve, manipulate, or destroy data. By removing the capabilities that you do not need to perform your business activities, you lessen the chance that your business data will be inappropriately accessed, stolen, or worse.

Consider another example. Many applications have many different predefined privileges based upon user group or role authorization. However, often organizations do not assign roles granularly enough, lumping an entire department under one role because it is easier and quicker to do. That one role, however, is often one that can do a very wide range of actions leading to inadequate separation of duties privileges. As a result, there is no accountability or ability to perform per user authorization. There is also the very real possibility that fraud can occur by one of the users figuring out that, for instance, he can not only request a check but also approve the request and indicate to which address (one he has set up) it should be sent. Bottom line: If you do not need some of the application's capabilities, get rid of them.

Internet-Facing Applications Security Improvement Checklist

So, as a quick review, when developing and deploying Internet-facing applications:

- Incorporate security into the application throughout the entire development process
- Use a positive security model to establish access capabilities
- Provide granular access to applications
- Restrict applications' capabilities; disable those you do not need

These four actions will dramatically improve your applications' security capabilities and help to protect your business data.

Article 9: Using Certified Products to Improve Compliance

What Does “Certified” Really Mean?

Over the past few years, there have been a slew of security certifications that have sprung up professing to validate that the security product you are buying has been independently vetted to validate that it is trustworthy and will not create more vulnerabilities than it closes if you implement it within your enterprise. Table 1 provides a listing of a few of the better-known such certifications.

Certification	What It Means
Common Criteria (CC) Certification	From the Common Criteria site (http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf): “The CC presents requirements for the IT security of a product or system under the distinct categories of functional requirements (CC Part 2) and assurance requirements (CC Part 3). The CC functional requirements define desired security behaviour. Assurance requirements are the basis for gaining confidence that the claimed security measures are effective and implemented correctly.”
ISO/IEC 27001 Certification	From BSI Global (http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=00000000030126472&recid=253): “BS ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) and specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system (ISMS) within the context of the organization’s overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations. The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. If an organization already has an operative business process management system (e.g. in relation to ISO 9001 or ISO 14001), it is preferable in most cases to satisfy the requirements of this International Standard within the existing management system.”
NSS Group Certification	From NSS (http://www.nss.co.uk/aboutnss.htm): “The NSS Group awards are recognised world-wide as being the most desirable and essential when it comes to security products. Vendors consider the awards to be a crucial step in any security-related marketing campaign, whilst feedback from readers of the reports indicates that participation in an NSS Group test and/or one of the NSS Approved awards is a prerequisite for any security product in order to be considered for purchase.”
FIPS-140	From NIST (http://csrc.nist.gov/cryptval/): “Security requirements cover 11 areas related to the design and implementation of a cryptographic module. Within most areas, a cryptographic module receives a security level rating (1-4, from lowest to highest), depending on what requirements are met. For other areas that do not provide for different levels of security, a cryptographic module receives a rating that reflects fulfillment of all of the requirements for that area.”
Cybertrust Certification	From Cybertrust (http://www.cybertrust.com/media/data_sheets/cybertrust_ds_certifications.pdf): “Created in 1997, Cybertrust offers the most mature certification program in the industry, with the largest customer base. We have programs to certify your enterprise, perimeter or locations. Or we can help you build your own certification program to ensure your partners, vendors and business units are meeting your standards.”

CIS Software Certification	From CIS (http://www.cisecurity.org/trademarks.html): “The CIS Software Certification Mark signifies that a security software product has been: (1) tested to accurately measure and report the conformity of computer configurations with the technical settings and actions defined in the CIS Security Benchmark and (2) awarded Certification by CIS.”
BITS Certification	From BITS (http://www.bitsinfo.org/c_certification.html): “The BITS Product Certification Program tests technology products used to deliver financial services at unbiased and professional facilities against minimum-security criteria established by the financial services industry.”

Table 1: Sample security certifications.

However, there has also been much discussion and wide debate about how useful these certifications are. The value of these certifications really depends upon the scope of the certification, the goal the organization has for getting a certification, and the true independence of the certifying organization. Each of these certifications is achieved through its own evaluation process for certification.

Does Certification Really Mean You Have a Better Product?

In general, it is always a good thing to know that there has been an independent review of a security product prior to committing to the purchase. The key is to ensure qualified and truly non-biased reviewers performed the certification process, and that the certification was not obtained just by paying enough money for it.

I am skeptical of many vendor-specific certifications; some seem as though the only real benefit is to the vendor that is offering the certification as another revenue stream for their company, which weakens their objectivity. After all, if a vendor wants to sell as many of their certifications as possible to bump up their revenue, they are likely to not be as stringent as an organization—such as one of those providing certification for the Common Criteria—that is providing certification as a way to provide an internationally accepted methodology to validate the security of software.

Different Certifications = Different Meanings


A growing number of commercial firms and independent consultants offer impartial security assessment or audit services for software applications and systems. They range from a series of reviews, tests, and assessments throughout the software life cycle to focusing on post-development penetration testing, vulnerability scanning, and software security audits. Some software security testing tool vendors also offer testing and certification services, but the caveat is that the tests must be performed using their tools. Accredited vendors who use the independent security assurance methodologies, such as the Common Criteria, will provide assurance that they are using proven and accepted international methodologies to validate the security of software.

Other security certifications exist that are very specific to a particular security issue, such as FIPS-140 certification of cryptographic software. Cybertrust provides multiple certifications, including one for application security, one for the enterprise, and another for the network perimeter. Center for Internet Security (CIS) is a non-profit organization that uses benchmarking practices to evaluate security for systems and networks. BITS is for use only within the financial industry and strives to establish a validated set of security practices for banking and financial services with what they indicate is a simpler certification process than that of the Common Criteria.

As they apply to all types of organizations and are based upon accepted international standards and methodologies, let's look more closely at the Common Criteria certification to validate the security of products, and the ISO/IEC 27001 certification to provide validation for the vendor organization itself.

Common Criteria


If a product is Common Criteria certified, does that mean it is completely secure? Not necessarily.

 The criteria are "common" in that they are shared internationally as the result of agreement among a number of countries that formerly had differing security criteria.

The Common Criteria is the most widely referred to international standard for evaluating software products and systems with significant security functionality. In the U.S., the Common Criteria consists of a two-step process:


1. Evaluation by an approved laboratory/vendor and then,
2. Validation by the government.

The assignment of Evaluation Assurance Level (EAL) ratings 1 through 4 is done by the National Information Assurance Partnership (NIAP) and EAL levels 5 through 7 are generally done by the National Security Agency (NSA). A number of countries have a reciprocity agreement for EAL levels 1 through 4.

 EAL is the numerical rating assigned to the target of the evaluation (such as a specific application or system) that reflects the depth of the assurance requirements met during the evaluation. Each EAL corresponds to a set of requirements covering the complete development of a product as it corresponds to a given level of security strictness. Common Criteria lists seven levels, with EAL1 being the most basic, least restrictive, and cheapest to implement and evaluate. EAL7 is the most stringent and most expensive. Higher EAL levels do not necessarily mean the software has "better security;" it means the security has been more extensively validated.

The Common Criteria contains:


- Enumeration of security functionality and capabilities, such as authentication and logging
- EAL 1 (low) through 7 (high), calling for increased levels of documentation, formality, and testing as the level numbers increase
- Consistent methods that must be followed by those doing the evaluation and certification

 The Common Criteria provides a global security standard that can assure those using them of consistent testing rigors and demonstrated levels of security capabilities.

Knowing that a security software product has obtained a Common Criteria certification provides assurance that it was truly independently analyzed. Be sure you are aware of the scope of the certification, and remember that the higher the EAL level, the more security validation that occurred to obtain certification.

Common Criteria certification tells the organizations using them that the applications and systems:


- Have been engineered to protect the applications and systems from compromise and unauthorized use
- Were tested and validated to the EAL level indicated; with the higher levels meaning more validations and testing occurred
- Were engineered according to a specific protection profile standard consisting of a standard minimum set of security requirements

 A protection profile is an independent set of security requirements for a specific category of IT products that meet specific consumer and user needs.

 For a list of CC evaluated products see <http://www.commoncriteriaportal.org/public/consumer/index.php?menu=5>.


ISO/IEC 27001 Certification

Whereas Common Criteria certifies the security capabilities of software and systems, ISO/IEC 27001 certification certifies the information security program and practices of an organization. ISO/IEC 27001 provides an international standard for organizations to use to establish, implement, operate, monitor, review, maintain, and improve upon their clearly defined Information Security Management System (ISMS).

 An ISMS includes the organizational structure, policies, planning activities, responsibilities, practices, procedures, processes, and resources.

An ISMS encompasses the entire information security program and must integrate with and relate to all other parts of the enterprise. ISO/IEC 27001 lists the various organizational functions required for security certification, including a list of required documents that must be maintained and provided for review during the certification process.


ISO/IEC 27001 applies to all types of organizations. The prescribed ISMS must be established to be appropriate for the organization's risk level and overall risk management processes. ISO/IEC 27001 certification provides validated assurance that an organization has implemented the part of their security program that is encompassed by the scope of the ISMS certification in compliance with their own documented program. Authentic ISO/IEC 27001 certification can only be performed by accredited certification organizations and auditors.

 As of March 2007, 3350 organizations throughout the world had achieved ISMS certification. See <http://www.iso27001certificates.com/> for more information about those with ISMS certification along with a listing of accredited ISMS auditors and organizations.

Certification Assists with Compliance Efforts

The independent review of the security worthiness of software products and the associated product vendors is becoming so important that it is starting to show up more often within requests for proposals (RFPs) for vendor security products. Because virtually all organizations must now provide documented proof that they are appropriately safeguarding information to effectively minimize risks to an acceptable level to meet related compliance requirements, the certification helps to demonstrate that the organizations are following a standard of due care with regard to their software choices.

Not only must organizations implement secure applications for regulatory compliance, they increasingly must do so to comply with the requirements of their business partners. This compliance goes beyond just describing the security products they are using; it requires that the organizations provide documented proof that they have acceptable security in place. One such method of providing this proof is by using a certified security product.

 As organizations face compliance obligations and are expected to implement internationally accepted standards to safeguard information assets, there will be more emphasis on certification and accreditation of security prior to applications or systems implementation.

The most effective way to ensure secure applications and systems is through a continuous assessment process to manage risk and compliance with standards and regulations. Throughout the world, ISO/IEC 27001 has become the de facto standard for defining at a high level an effective ISMS. The Common Criteria product certification is becoming more widely pursued and recognized, especially as more organizations require such certification to use the products.



The U.S. Department of Defense agencies mandate that security products considered for purchase must be Common Criteria certified.

Certified security products provide independent validation that software applications and systems satisfy specific security requirements relevant to a number of regulations and business partner contracts. Certain certifications, such as the Common Criteria, provide documentation and, in effect, an audit trail of the engineering considerations—from requirements to full evidence of compliance. They provide the justification of why certain security processes were, or were not, implemented and provide documented descriptions of how they were judged to be successfully effective. Such documentation and evidence can be very helpful when trying to demonstrate compliance to a regulatory auditor and could cut the time of the audit dramatically.